

IEEE 802.11g 54Mbps Wireless Bridge

Dolphin-M

User's Manual

V1.0.0

Copyright

There is no any clear or implicit assurance in the user's manual of our company, including the assurance of selling or installing for the special purpose. There are rival's volumes to carry on the power to alter or revise in our company, if alter and forgive me for not issuing a separate notice. You can't duplicate any content of this manual by the written permission of our company.

About the manual

The purpose to use this manual is for install the wireless bridge. This manual is including disposing course and method and helping the customer to solve the unpredictable problem.

Chapter 1 Introduction

Introduction

Thank you for choosing 802.11b/g Ethernet-to-Wireless Bridge—Dolphin-M. Dolphin-M is an IEEE 802.11g standard wireless bridge enabling a laptop, pc or embedded device with Ethernet port without build-in wireless capability to connect to a wireless LAN. It delivers a 54Mbps high speed and fully compliant with 802.11b & 802.11g standard, and could easily be changed to support 802.11a standard by inserting the 802.11a compliant mini-PCI wireless module, it has two working mode: Infrastructure and Ad-hoc.

Dolphin-M provides both basic 64/128-bit WEP encryption and Wi-Fi Protected Access(home WPA, professional WPA2). It's completely driver-free, so it works on any platform and under any operating system! Since there's no drivers to load, setup is a snap—configure the network settings through your PC's web browser, then plug it into your device and go, it also has the ability to be configured through your device's Ethernet port.

Dolphin-M provides highly stable, secure, flexible and reliable wireless connection. This guide shows you how to setup and connect Dolphin-M wireless bridge to your wireless LAN.

Appearance of product

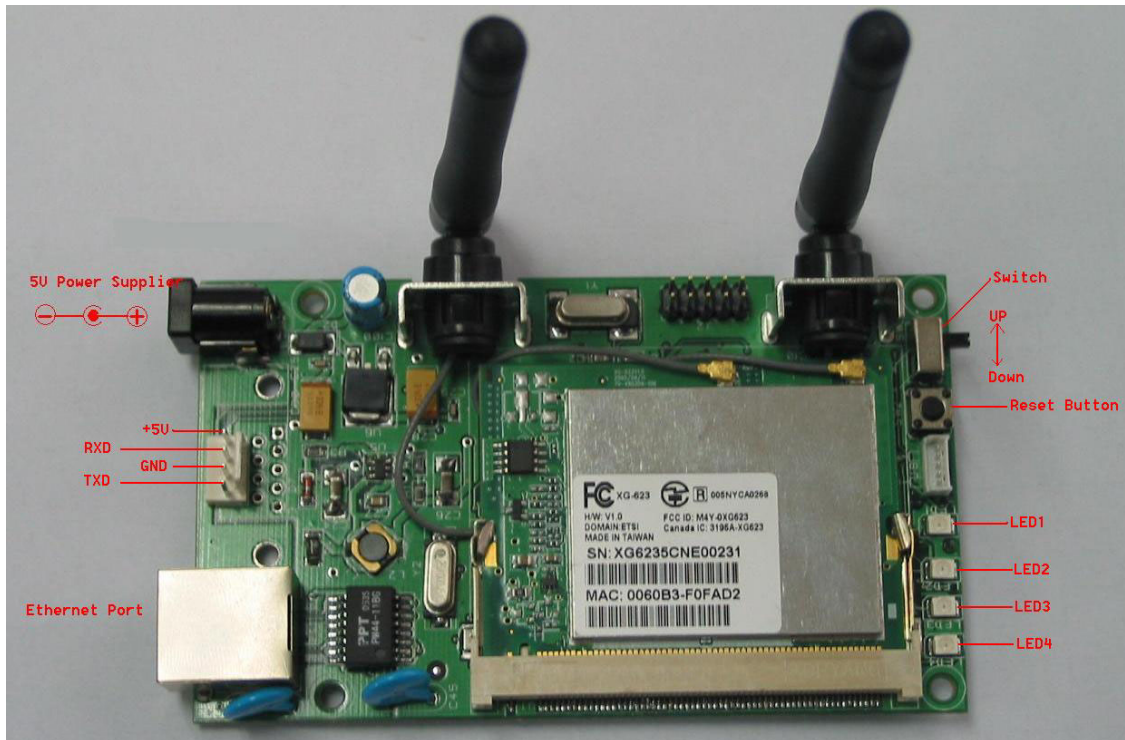


Figure 1 Appearance of Dolphin-M

LED mechanical description

LED num	LED definition	status	Description
LED1	POWER	Red	Power enabled
LED2	WLAN	Red	Flashing slowly: Scan AP
			On : No wireless LAN traffic activity
			Flashing quickly: Wireless LAN traffic activity
LED3	LAN	Red	On: No wired LAN activity
			Flashing : Wired LAN traffic activity
LED4	Mini-PCI module	Red	On: mini-PCI wireless module enabled
			Off: mini-PCI wireless module disabled

Features and benefits

- **High Speed & Backward Compatible:** The high-speed device simultaneously supports both IEEE 802.11b/g 54Mbps wireless networks.
- **Compliant with IEEE 802.3/802.3u wired Ethernet network protocol,** auto identify MDI/MDIX's 10M/100M Ethernet port.
- **Support two wireless working modes:** Infrastructure and ad-hoc.
- **Support MAC clone function.**
- **Supports static IP address or DHCP client to obtain IP address from DHCP server automatically.**
- **Provide the highest available security level of WEP, WPA and WPA2.**
- **Auto select the suitable speed of 1, 2, 5.5, 6, 9, 11, 12, 18, 22, 24, 36, 48, 54Mbps to let the network quality stay in best condition.**
- **Support WEB management and update, and also support configuration through Ethernet port.**
- **Dynamic LED indicator, provide simple working state indication and troubleshooting.**
- **Display AP list in the range of activity.**

Application

- **Remote access to corporate network information**
E-mail, file transfer and terminal emulation.
- **Difficult-to-wire environments**
Historical or old buildings, and open area where wiring is difficult to deploy.
- **Frequently changing environments**
Retailers, manufacturers and those frequently rearrange the workplace and change location will use this.

- Temporary LANs for special projects or peak time

Trade shows, exhibitions and construction sites where a temporary network will be practical. Retailers, airline and shipping companies need additional workstations during peak period; Auditors requiring workgroups at customer sites.

- Access to database for mobile workers

Doctors, nurses, retailers, accessing their database while being mobile in the hospital, retail store or office campus.

- SOHO (Small Office and Home Office) users

SOHO users need easy and quick installation of a small computer network.

- High security connection

The secure wireless network can be installed quickly and provide flexibility.

Chapter 2 Basic configuration

Default settings

As you are the first time to use the bridge, you'll see the default settings as the following table. You can also restore the default settings, please refer to “**Restore to Factory Defaults**” for detailed method.

Diagram 2 Default Settings

Options	Default Value
User	admin
Password	password
Bridge Name	802.11b/g Bridge
Working mode	Infrastructure
SSID	ZQNET
Rate	Best(Automatic)
802.11 mode	Mixed 802.11g and 802.11b
Channel	Auto(Follow AP)
Network Authentication	Open (Auto)
Data Encryption	Disable
Address Clone Mode	Wireless module
RTS Threshold	2346
Fragment Threshold	2346
Beacon Interval	100 ms
Transmit Power	High
Antenna Selection	Auto Switch
IP Setting	DHCP Client: Disable Default IP address: 192.168.0.60 Subnet Mask: 255.255.255.0 Default Gateway:192.168.0.1

Using the WEB management

The WEB management offers a friendly user's interface. You can look into and configure the device through the browser.

1. First activate the IE, and type the default IP:

<http://192.168.0.60>

Notice:

Please set the IP Net segment of the PC adapter to the same as the bridge.

2. Enter the login windows, input the default user name and password, press "OK" button, then you can enter the main page and set the device.

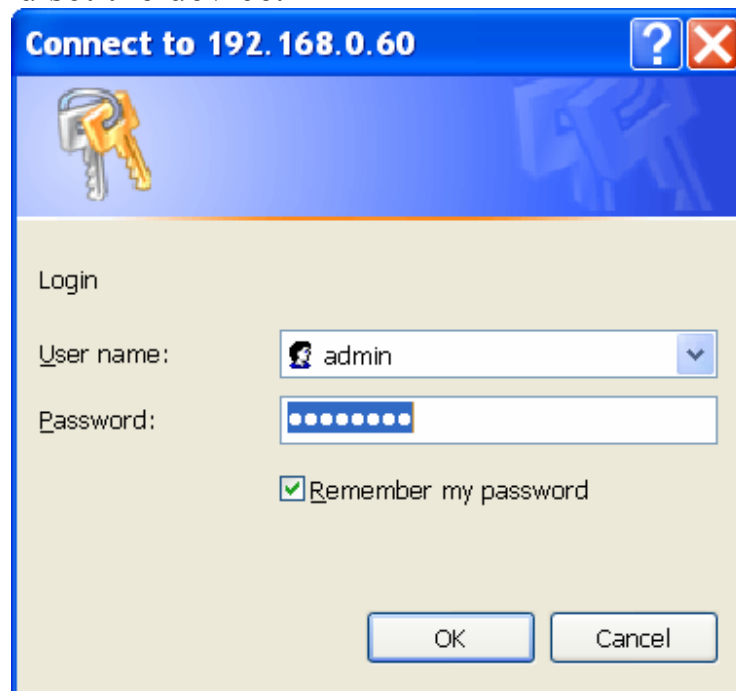


Figure 2 Login page

3. After you login successfully, you will see the main page as follows:

Dolphin-M User's Manual

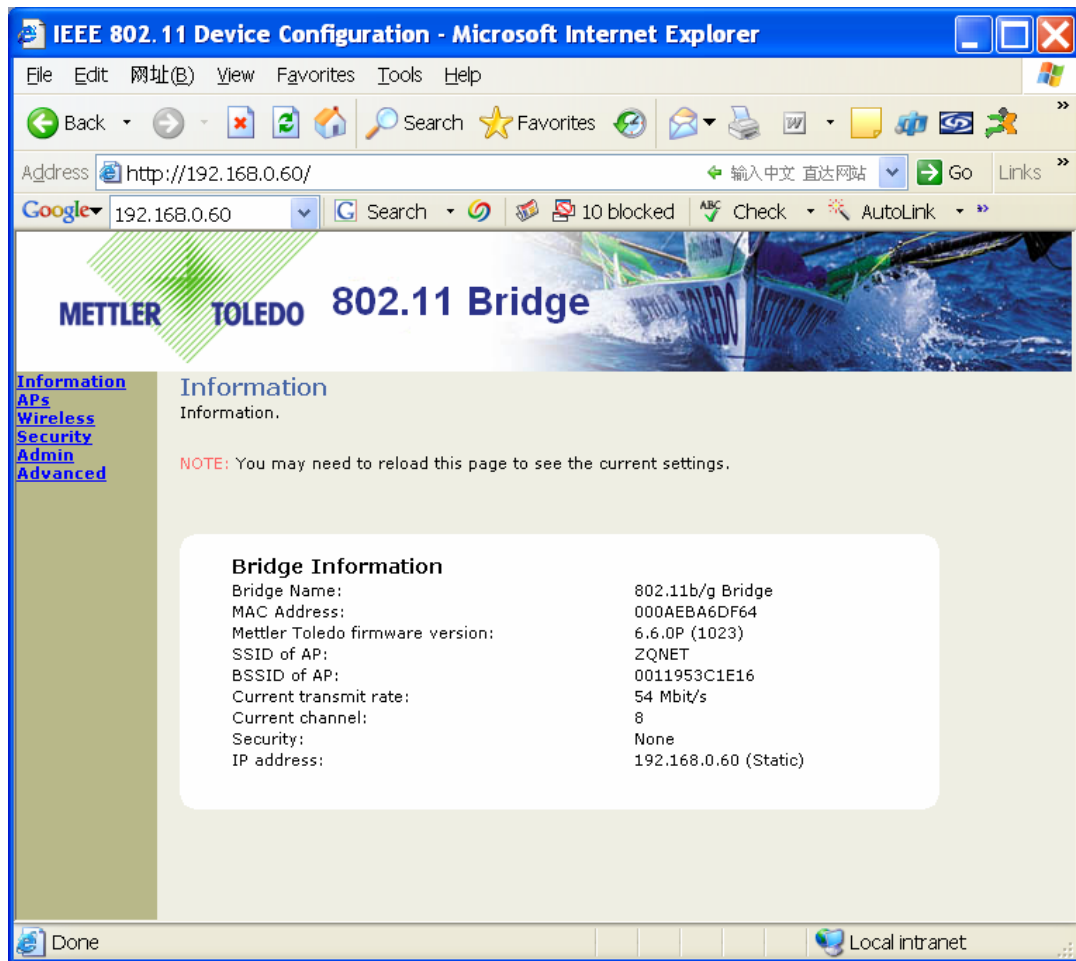


Figure 3 Main Page

Set the Basic Wireless Parameters

Press the item “[Wireless](#)” on the left column, and you can set the Basic Wireless Parameters.

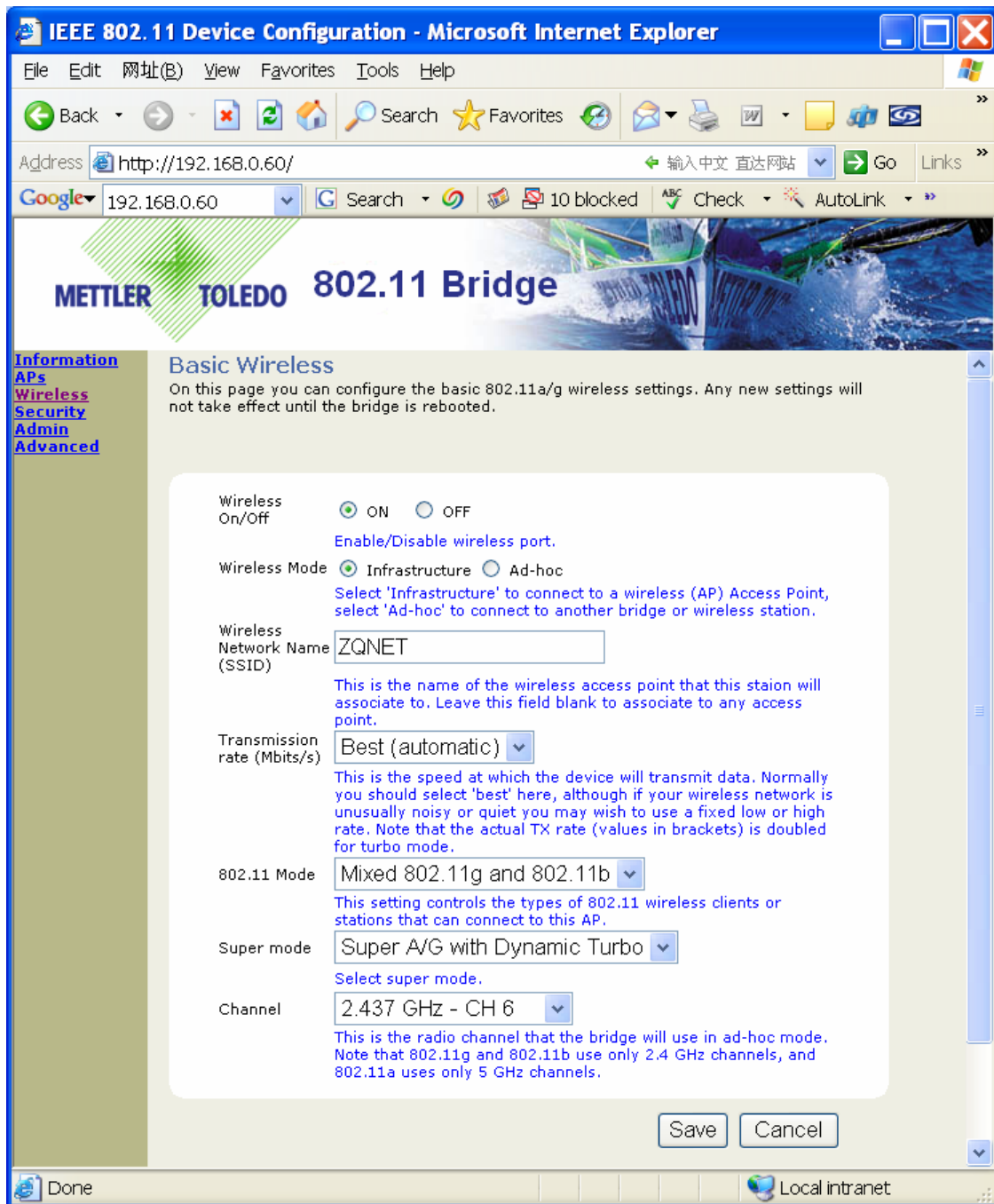


Figure 4 Basic wireless

●Wireless On/Off

On — Enable wireless port(Default)

Off — Disable wireless port

●Wireless Mode

There are two wireless modes for the bridge to operate. If you need to access company network or Internet via an Access Point, select “**Infrastructure**”. To set up a group of wireless stations for files and printer sharing, select “**Ad-Hoc**” (without Access Point). For Ad-Hoc operation, the same ESSID is required to set for the wireless stations.

●Wireless Network Name(SSID)

The SSID is a unique ID used by Access Points and Stations to identify a wireless LAN. Wireless clients associating to any Access Point must have the same SSID. The default SSID is “**ZQNET**”. The SSID can up to 32 characters.

●Transmission Rate

Transmission rates options include Best(automatic), 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48 and 54Mbps. The default setting is automatic.

●802.11 Mode

There are four different 802.11 wireless modes to operate, “**802.11b only**”, “**802.11g only**”, “**Mixed 802.11g and 802.11b**”, and “**802.11a only**”. In 802.11b/g mixed mode, the bridge is compatible with a mix of both 802.11g and 802.11b AP. **The 802.11a mode is only valid when compliant 802.11a mini-PCI wireless module is deployed.**

●Super mode

There are four super mode options to select, “Disabled”, “Super A/G without Turbo”, “Super A/G with Static Turbo” and “Super A/G with Dynamic Turbo”, the last three modes need the support of corresponding wireless module.

- **Channel**

Only need to configure the channel when the bridge works in Ad-hoc mode, when the bridge works in infrastructure mode, the channel is auto running after the AP's.

Chapter 3 Security Configuration

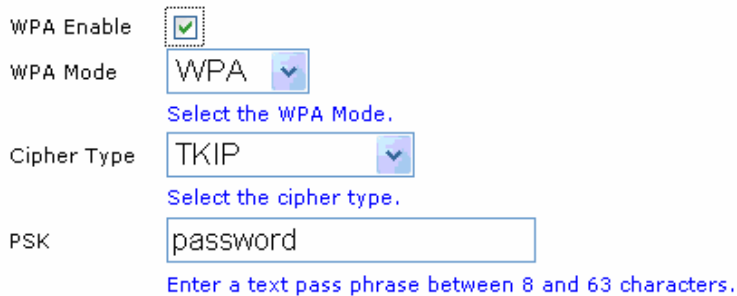
Security Setup

You can press the item “**Security**” on the left column to configure the wireless security parameters to enhance the security of the wireless network.

WPA setup

WPA configuration

Enable WPA Authenticator to require stations to use high grade encryption and authentication.



The screenshot shows a WPA configuration interface with the following fields and options:

- WPA Enable:** A checkbox that is checked.
- WPA Mode:** A dropdown menu currently set to "WPA". Below it is a blue link that says "Select the WPA Mode."
- Cipher Type:** A dropdown menu currently set to "TKIP". Below it is a blue link that says "Select the cipher type."
- PSK:** A text input field containing the word "password". Below it is a blue link that says "Enter a text pass phrase between 8 and 63 characters."

Figure 5 WPA setup

●WPA Enable

Check the box to enable WPA security if you use the WPA for the wireless data encryption.

●WPA Mode

WPA — WPA home

WPA2 — WPA professional

●Cipher Type

There are three cipher types to be selected:

TKIP — Temporal Key Integrity Protocol

AES — Advanced Encryption Standard

TKIP+AES

●**PSK(Pre-Shared Key)**

The length of PSK should be 8~64 characters.

WEP setup

WEP configuration

WEP is the wireless encryption standard. To use it you must enter the same key (s) into the bridge and the access point. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. If you leave a key box blank then this means a key of all zeros.

Enable WEP	<input checked="" type="checkbox"/>	Check this box to enable WEP. For the most secure use of WEP, also set the authentication type to "Shared Key" when WEP is enabled
Default WEP key to use	WEP Key 1 ▼	Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
Authentication	Open ▼	Select the type of authentication used when connecting to an access point. 'Open' is used if anyone can connect to the AP. 'Shared key' is used if both devices must know the encryption key.
WEP key lengths	64 bit (10 hex digits) ▼	Select the WEP key size. This length applies to all keys.
WEP key 1	<input type="text" value="••••••••••"/>	
WEP key 2	<input type="text" value="••••••~••••"/>	
WEP key 3	<input type="text" value="••••••~••••"/>	
WEP key 4	<input type="text" value="••••~••••••••"/>	

Figure 6 WEP setup

●**WEP Enable**

Check the box to enable the WEP security if you use the WEP for the wireless data encryption.

●**Default WEP key to use**

You can select one of the four WEP keys to be used as the default key.

●**Authentication**

There are two types of authentication: Open, Shared Key.

Open — It requires no authentication since it allows any device to join a network without performing any security check.

Shared Key — It provides higher security for wireless access. **Note that when Shared Key is selected, a WEP key is required and must be the same between the Access Point and client.**

● **WEP key lengths**

64 bit(10 hex digits) — Requires the wireless bridge to use data encryption with 40-bit algorithm when communicating with the Access Point.

128 bit(26 hex digits) — Requires the wireless bridge to use data encryption with 104-bit algorithm when communicating with the Access Point.

● **WEP key**

You may enter 10(64 bit WEP) or 26(128 bit WEP) **hexadecimal digits** in the range of “A-F”, “a-f” and “0-9” into the box of default WEP key, and the same length digits to others or keep other key empty.

Chapter 4 Advanced Configuration

Advanced Wireless Parameters

You can press the item “Advanced” on the left column to configure advanced wireless parameters.

Cloning

Cloning mode ☒ WLAN Card ☐ Ethernet Client

This feature controls the MAC Address of the Bridge as seen by other devices (wired or wireless).

If set to "Ethernet Client", the MAC Address from the first Ethernet client that transmits data through the Bridge will be used. This setting is useful when connected to an Xbox or if there is only one Ethernet device connected to the Bridge. When multiple Ethernet devices are connected to the Bridge, it may not be obvious which MAC Address is being used.

If set to "WLAN Card", the MAC Address of the WLAN Card (typically written on the back of the card) will be used. When multiple Ethernet devices are connected to the Bridge, the MAC Address of the Bridge will not change.

Advanced wireless

Fragmentation threshold

Transmitted wireless packets larger than this size will be fragmented to maintain performance in noisy wireless networks. The valid range is 256..65535. Values larger than about 1560 will prevent fragmentation from taking place.

RTS threshold

Transmitted wireless packets larger than this size will use the RTS/CTS protocol to (a) maintain performance in noisy wireless networks and (b) prevent hidden nodes from degrading performance. The valid range is 1..65535. Values larger than about 1560 will prevent RTS/CTS from taking place.

Beacon period

In adhoc mode beacons are sent out periodically. This is the number of milliseconds between each beacon. The valid range is 20..1000.

802.11d

☐

Check this box to enable support for receiving regional information from the access point.

Transmit Power

Select Antenna Transmit Power.

Antenna selection

Select antenna of non-MiMo radios for testing. The valid values are 0(auto-switching), 1(antenna 1) and 2(antenna 2).

Figure 7 Advanced wireless

MAC address clone

Controls the MAC address of the bridge as seen by other devices, there are two options to the cloning mode: WLAN card, Ethernet client. If set to “WLAN card” (default), the MAC address of WLAN card will be used, if set to “Ethernet client” , the MAC address from the first Ethernet client that transmits data through the bridge will be used.

Advanced wireless

●Fragmentation threshold

Fragmentation mechanism is used for improving the efficiency when there is high traffic within the wireless network. If you transmit large files in a wireless network, you can enable the Fragmentation Threshold and specify the packet size.

●RTS threshold

RTS threshold is a mechanism implemented to prevent the “hidden node” problem. “Hidden node” is a situation in which two stations are within range of same Public Access Point, but are not range of each other. Therefore, they are hidden nodes for each other. When a hidden station starts data transmission with the Public Access Point, it might not notice that another station is already using the wireless medium. When these two stations send data at the same time, they might collide when arriving simultaneously at the Public Access Point. The collision will most certainly result in a loss of messages for both stations. Thus, the RTS threshold mechanism will provide the solution to prevent data collisions. When the RTS threshold is activated, the station and its Public Access Point will use a Request to Send/Clear to Send protocol (RTS/CTS). The station will send an RTS to the Public Access Point, informing that it is going to transmit the data. Upon receipt, the Public Access Point will respond with a CTS message to all stations within its range to notify all other stations to defer transmission. It will also

confirm to the requesting station that the Public Access Point has reserved the channel for transmission.

- **Beacon period**

The amount of time between beacons in kilo microseconds.

- **802.11d**

Enable the support for receiving the regional information from Access Point.

- **Transmit Power**

There are three level of transmit power: High (default), Medium and Low. Under default status – high transmit power, gain the more wide range; Set to Medium or Low transmit power may reduce the radiation to the circumstance.

- **Antenna selection**

There are three antenna working mode: Use antenna diversity (default), Use antenna #1 and Use antenna #2.

Chapter 5 Management

View the basic information

Open the page of “**Information**”, you can see the basic information of the wireless bridge, such as Bridge Name, MAC address, Link status, MAC address of the AP, etc. All the information on the page is read-only.

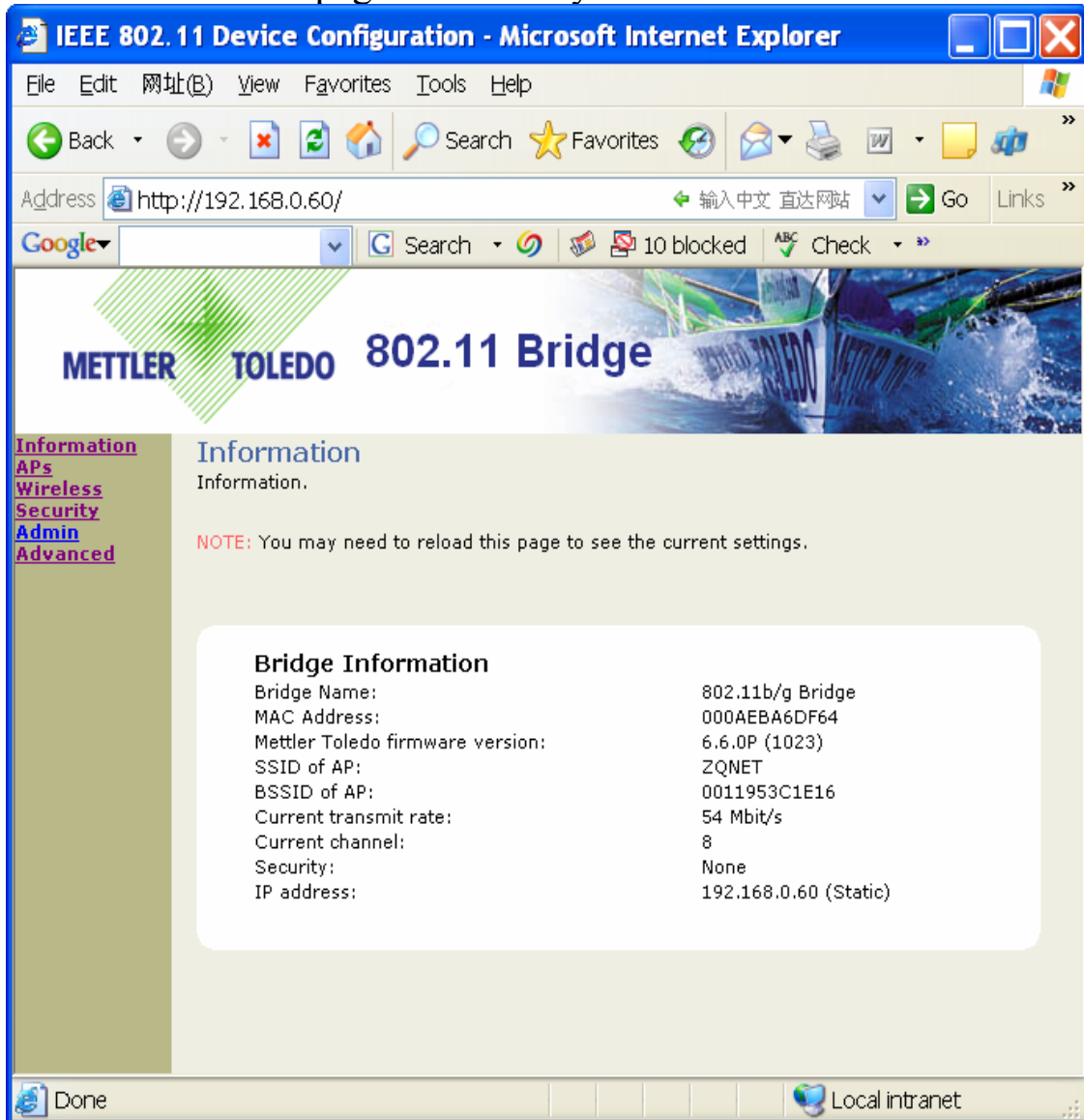


Figure 8 General Information of the wireless bridge

View the AP list

Open the page of “APs”, you can check the status of around available networks within the range of the wireless bridge, it includes the MAC address, SSID, Channel, Mode, Rate and RSSI(Received Signal Strength Indication).

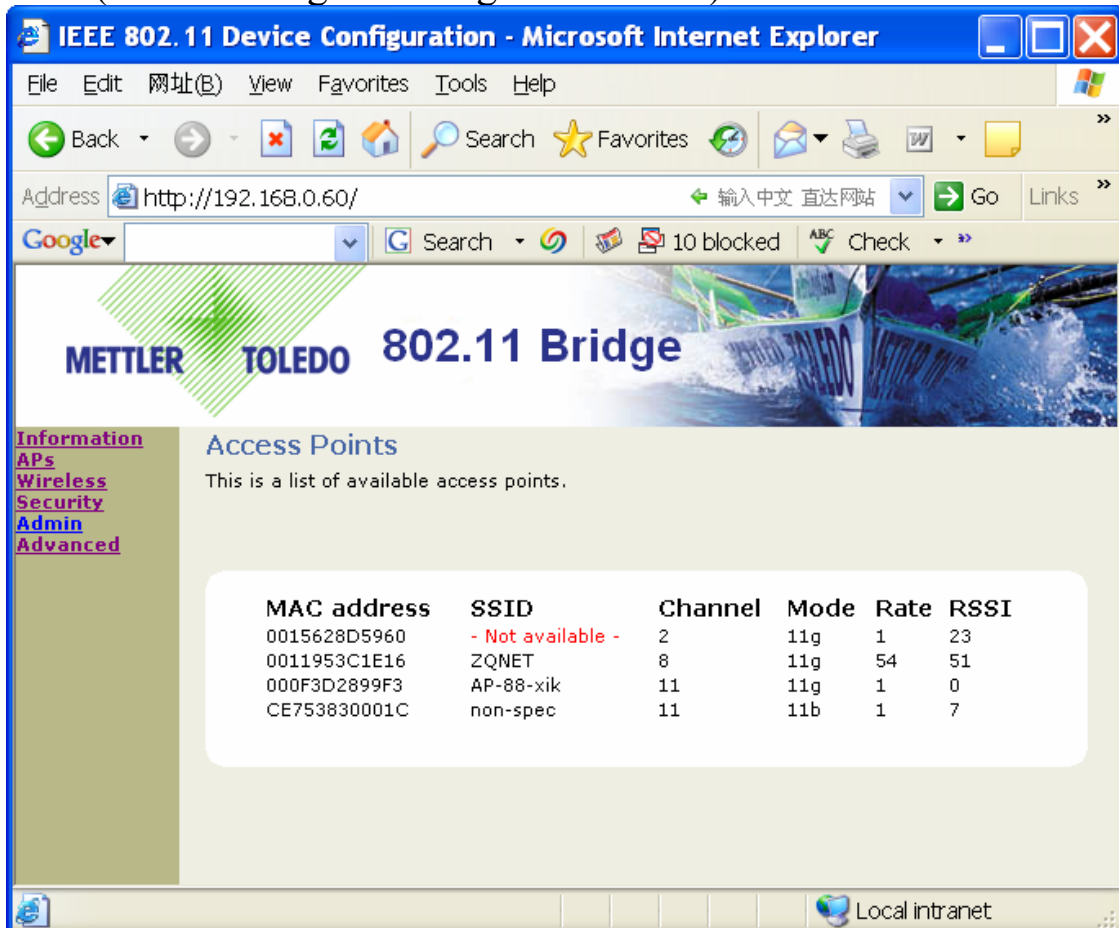


Figure 9 AP Information within the range of the wireless bridge

Device Control and Management

Open the page of “Admin” on the left column, you can control and manage the wireless bridge.

Device Control

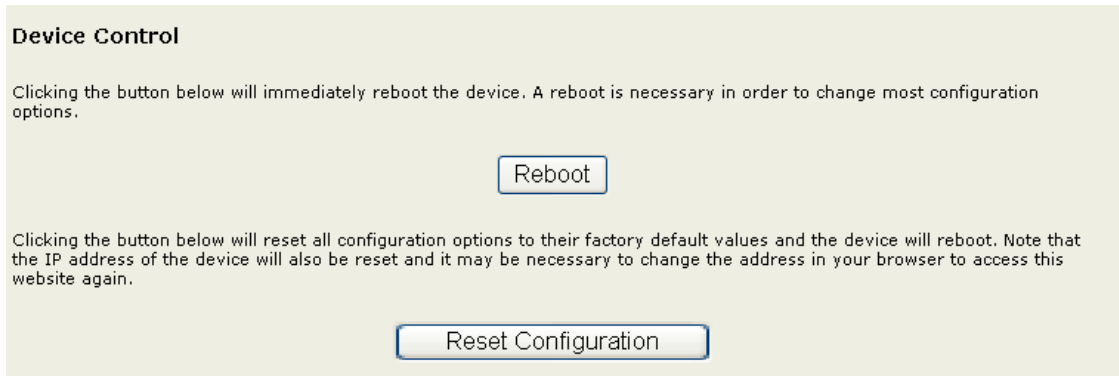


Figure 10 Device Control

- Click the “**Reboot**” button, you can reboot the device.
- Click the “**Reset Configuration**” button, you can reset all configurations to their factory default values and reboot the device.

Firmware upgrade

- You could upgrade the firmware of the device via WEB.

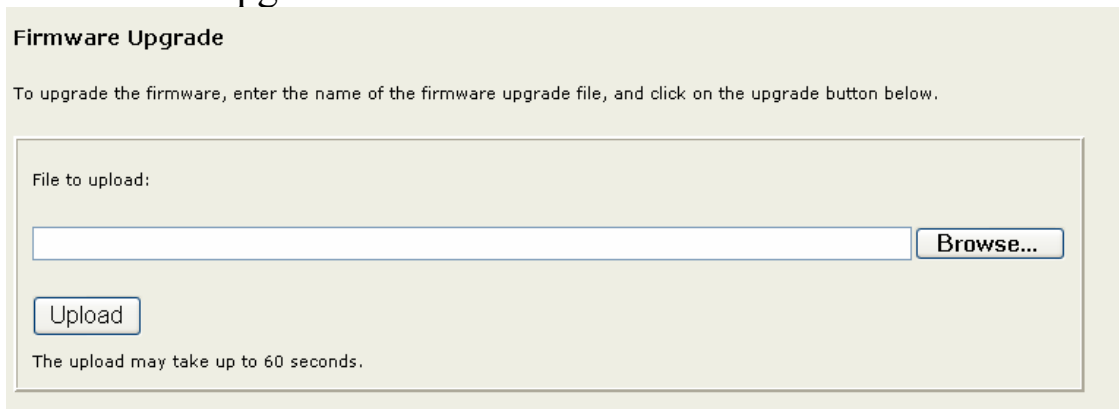


Figure 11 Firmware upgrade

1. Click the “**Browse...**”, and choose the file to upgrade.
2. Click the “**Upload**” to send the software into device.
3. Device will auto rebooting after the firmware upgraded.
4. Login again, turn to the page “Information” to make sure to make sure the upgrade successfully or not.

Warning:

While upgrading the firmware, do not power off the device or the computer! It must go until finish the reboot.

Device Name, IP settings and Access Control

The screenshot shows a web-based configuration interface for a Dolphin-M device. It is divided into three main sections: Device name, IP settings, and Security.

Device name

Device name:
This is the name that the bridge will use to identify itself to external configuration and IP-address-finding programs. This is not the same as the SSID. It is okay to leave this blank if you are not using these programs.

IP settings

IP Address Mode: ☒ Static ☐ DHCP
Select 'DHCP' to get the IP settings from a DHCP server on your network. Select 'Static' to use the IP settings specified on this page.

Default IP address:
Type the IP address of your bridge

Default subnet mask:
The subnet mask specifies the network number portion of an IP address. The factory default is 255.255.255.0.

Default gateway:
This is the IP address of the gateway that connects you to the internet. The factory default is 192.168.1.1.

Security

User name:
This is the user name that you must type when logging in to these web pages.

Administrator password:

This is the password that you must type when logging in to these web pages. You must enter the same password into both boxes, for confirmation

At the bottom right, there are two buttons: and .

Figure 12 Device name, IP settings and Security

- Up to 19 characters are valid or leave it blank when changing the device name.
- IP settings
 - ▶ Set the static IP address, Subnet mask and Gateway manually.
 In general, you could use 255.255.255.0 as the subnet mask.
 - ▶ Enable DHCP client
 The device could obtain IP address, Subnet Mask and Gateway from the DHCP server.

Notice:

You could use former used IP address to access the device, while obtaining IP address unsuccessfully.

- You could change the user name and password to login to the device next time, their all have the limited length of 15 characters.
- Click “Save” button to store the changes and reboot the device to activate the changes.

Restore to Factory Defaults

- Back to default setting via Web:
Open the page of “**Admin**”, and click “Reset Configuration” button, then the bridge reboot and back to default settings.
- Back to default setting via hardware Default Button:
Set the switch to “**UP**” state on Figure 1, hold on the “**Reset**” button at least 5 seconds then release, after about 5 seconds, the light LED2(WLAN) turn off then flash, the operation is successful.

WBCP Management

- You may also manage and configure the bridge by sending packets complying with WBCP(Wireless Bridge Configuration Protocol) protocol through the Ethernet port of your device.